Общество с ограниченной ответственностью
«СПСР - ЭКСПРЕСС»

Приложение 1 к Приказу № __19-рг_____ от ___30.07.2013_____

УТВЕРЖДАЮ
Генеральный директор
ООО «СПСР-ЭКСПРЕСС»
_____ *В.М. Солодкин*
«_30__» _____07_____ 2013 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ООО «СПСР-ЭКСПРЕСС»

Введен в действие
«_30___» _____07_____ 2013 г.
Приказ № _19-рг____ от «_30_»__07___2013 г.
Издание № 1

Москва 2013 г.

СОДЕРЖАНИЕ

ОСНОВНЫЕ ТЕРМИНЫ

Общество – ООО «СПСР-ЭКСПРЕСС».
Автоматизированная система – комплекс средств автоматизации, используемый для реализации информационной технологии.
Информационная технология – совокупность правил, приемов и методов применения средств вычислительной техники для выполнении функций хранения, обработки, передачи и использования финансовой, аналитической или другой связанной с функционированием Общества информации.
Доступность информации – свойство информационной системы, способное обеспечить своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.
Доступность данных – такое состояние данных, когда они находятся в виде, необходимом пользователю, в месте, и в то время, когда они ему необходимы.
Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах – библиотеках, архивах, фондах, банках данных и других информационных системах.
Информационные процессы – процессы сбора, обработки, накопления, хранения, поиска и распространения информации.
Информационная система – организационно упорядоченная совокупность документов, массивов документов и технологии обработки информации, в том числе с использованием средств вычислительной техники и связи, реализующей информационные процессы.
Информационная безопасность Общества – состояние защищенности информационных активов Общества в условиях угроз в информационной сфере.
Конфиденциальность информации – субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью информационной системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.
Мониторинг информационной безопасности Общества – постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности в Обществе, сбор, анализ и обобщение результатов наблюдения под заданные цели.
Управление информационной безопасностью Общества – совокупность целенаправленных действий, осуществляемых в рамках Политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления, выбор управляющих воздействий и их реализация.
Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности Общества при реализации угроз в информационной сфере.
Целостность информации - свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).
Целостность данных – состояние данных в вычислительной системе, когда они тождественны документам источника и не могут быть подвергнуты случайной либо умышленной модификации или уничтожению.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АС – автоматизированная система;
ЖЦ - жизненный цикл;
ИБ – информационная безопасность;
ЛВС – локальная вычислительная сеть;
НСД – несанкционированный доступ;
ОС – операционная система;
СКЗИ – средство криптографической защиты информации;
СУБД – система управления базами данных.
ЭВМ – электронная вычислительная машина;
ЭП – электронная подпись:

ВВЕДЕНИЕ

Политика информационной безопасности ООО «СПСР-ЭКСПРЕСС» определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Общество в своей деятельности.

Общее руководство обеспечением ИБ Общества осуществляет Первый заместитель генерального директора Общества. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет ведущий специалист по информационной безопасности.

Основные положения и требования данного документа распространяются на все структурные подразделения Общества, включая филиалы, обособленные подразделения и представительства. Основные вопросы Политики ИБ также распространяются на другие организации и учреждения, взаимодействующие с Обществом в качестве поставщиков и потребителей информационных ресурсов Общества в том или ином качестве.

Руководители подразделений Общества ответственны за обеспечение выполнения требований ИБ в своих подразделениях. Работники Общества обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией Общества, соблюдать требования настоящей политики и других документов ИБ.

Невыполнение работниками Общества требований ИБ приравнивается к невыполнению должностных обязанностей и приводит к дисциплинированной ответственности.

1. НАЗНАЧЕНИЕ И ПРАВОВАЯ ОСНОВА ДОКУМЕНТА

Политика информационной безопасности Общества определяет систему взглядов на проблему обеспечения безопасности информации и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации в Обществе.

Законодательной основой настоящего документа являются Конституция Российской Федерации, Гражданский и Уголовный кодексы, законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности, Федеральной службы по надзору в сфере связи и массовых коммуникаций.

Политика ИБ является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности информации в Обществе;
- принятия управленческих решений и разработки, практических мер по воплощению политики безопасности информации и выработки комплекса, согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;

- координации деятельности подразделений Общества при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению безопасности информации;
- разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения безопасности информации в Обществе.

При разработке Политики ИБ учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Основные положения политики не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

2. ОПРЕДЕЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Информационная безопасность – состояние защищенности информационных активов в условиях угроз в информационной сфере.

Угрозы могут быть вызваны: непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов Общества.

Защищенность достигается обеспечением совокупности таких свойств информационной безопасности как:
Конфиденциальность - доступ к информации только авторизированных пользователей;
Целостность - достоверность и полноту информации и методов ее обработки;
Доступность - доступ к информации и связанным с ней активами авторизованных пользователей по мере необходимости.

Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий и документов по управлению информационной безопасностью, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного обеспечения. Указанные мероприятия должны обеспечить достижение целей информационной безопасности Общества.

3. ЦЕЛИ И ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА

Главной ***целью*** информационной безопасности является обеспечение устойчивого функционирования Общества и защита информационных ресурсов, принадлежащих Обществу, партнерам и клиентам от случайных (ошибочных) и направленных противоправных посягательств, разглашения, утраты, утечки, искажения, модификации и уничтожения охраняемых сведений.

Основными ***целями*** Информационной Безопасности Общества также являются:
- повышение стабильности функционирования Общества в целом;
- достижение адекватности мер по защите от реальных угроз ИБ;
- предотвращение и/или снижение ущерба от инцидентов ИБ.

Основными ***задачами*** деятельности по обеспечению ИБ Общества являются:

- разработка требований по обеспечению ИБ;
- контроль выполнения установленных требований по обеспечению ИБ;
- повышение эффективности мероприятий по обеспечению и поддержанию ИБ;
- разработка и совершенствование нормативно-правовой базы обеспечения информационной безопасности;
- выявление, оценка и прогнозирование угроз информационной безопасности;
- защита информации от НСД.

4. ОБЪЕКТЫ ЗАЩИТЫ

Основными объектами системы ИБ в Обществе являются:

- информационные ресурсы с ограниченным доступом, составляющие коммерческую тайну, персональные данные или иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, а также открытая (общедоступная) информация, необходимая для работы Общества, независимо от формы и вида ее представления;
- процессы обработки информации в информационной системе Общества информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и обслуживающий ее персонал;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные элементы информационной среды.

Информационная система Общества объединяет информационные подсистемы Центрального офиса, филиалов, обособленных подразделений и представительств в единую информационную систему Общества.

К основным особенностям информационной системы Общества относятся:

- широкая территориальная распределенность компонентов информационной системы;
- объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;
- значительное расширение сферы использования автоматизированных систем обработки информации, широкое многообразие и повсеместное распространение информационно-управляющих систем в Обществе;
- большое разнообразие решаемых задач и типов обрабатываемых данных, сложные режимы автоматизированной обработки информации с широким совмещением выполнения информационных запросов различных пользователей;
- значительная важность и ответственность решений, принимаемых на основе автоматизированной обработки данных;
- объединение в единых базах данных информации различного назначения, принадлежности и уровней конфиденциальности;
- необходимость обеспечения непрерывности функционирования Общества;
- высокая интенсивность информационных потоков;
- разнообразие категорий пользователей и обслуживающего персонала системы.

В Обществе циркулирует информация различных уровней конфиденциальности, содержащая сведения ограниченного распространения (служебная, коммерческая информация, персональные данные), и открытые сведения. Владельцем информации являются подразделения, создавшие информационный ресурс. Уровень конфиденциальности устанавливается владельцами информационных ресурсов и информации.

Защите подлежит вся информация и информационные ресурсы Общества, независимо от ее представления и местонахождения в информационной системе Общества, а именно:

- сведения, составляющие коммерческую тайну, доступ к которым ограничен собственником информации в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации»;
- сведения о частной жизни граждан (персональные данные), доступ к которым ограничен в соответствии с Федеральным законом «О персональных данных»;
- открытая информация, необходимая для обеспечения нормального функционирования Общества.

5. ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

Субъектами информационных отношений при обеспечении информационной безопасности Общества являются:

- Общество, как собственник информационных ресурсов;
- подразделения Общества, участвующие в информационном обмене;
- руководство и работники структурных подразделений Общества, в соответствии с возложенными на них функциями;
- юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационной системе Общества;
- другие юридические и физические лица, задействованные в обеспечении выполнения Обществом своих функций (консультанты, разработчики, обслуживающий персонал, организации, привлекаемые для оказания услуг и пр.).

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- своевременного доступа к необходимой им информации (ее доступности);
- достоверности (полноты, точности, адекватности, целостности) информации;
- конфиденциальности (сохранения в тайне) определенной части информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации;
- разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
- защиты части информации от незаконного ее тиражирования (защиты авторских прав, прав собственника информации и т.п.).

Основной целью, на достижение которой направлены все положения настоящей Политики ИБ, является защита субъектов информационных отношений Общества от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация уровня операционного и других рисков (риск нанесения урона деловой репутации Общества, правовой риск и т.д.).

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

- доступности информации для легальных пользователей (устойчивого функционирования информационной системы Общества, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время);
- целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в информационной системе Общества и передаваемой по каналам связи;
- конфиденциальности - сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи;

Для достижения основной цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности Общества должна обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационной системы Общества;
- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования информационной системы Общества посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Общества (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- защиту от несанкционированной модификации используемых в корпоративной информационной системе Общества программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- обеспечение безотказной работы криптографических средств защиты информации.

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учетом всех подлежащих защите ресурсов информационной системы Общества (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);
- регистрацией в журналах действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы;
- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Общества по вопросам обеспечения безопасности информации;

- подготовкой должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;
- наделением каждого работника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Общества;
- четким знанием и строгим соблюдением всеми пользователями информационной системы Общества требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;
- персональной ответственностью за свои действия каждого работника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Общества;
- непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Общества;
- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
- эффективным контролем над соблюдением пользователями информационных ресурсов Общества требований по обеспечению безопасности информации;
- юридической защитой интересов Общества при взаимодействии его подразделений с внешними организациями (связанном с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

Приобретение и установка средств и систем защиты автоматизированных систем (средства защиты от несанкционированного доступа, антивирусные программы и пр.) осуществляются по согласованию с ведущим специалистом по информационной безопасности СБ.

Ввод в действие и снятие с эксплуатации систем защиты АС осуществляются при участии ведущего специалиста по информационной безопасности и уполномоченных работников Дирекции по информационным технологиям.

6. ОСНОВНЫЕ ВИДЫ УГРОЗ ОБЪЕКТАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Определение и прогнозирование возможных угроз и степени их опасности необходимы для обоснования, выбора и реализации защитных мероприятий.

Комплексный подход к проблеме защиты информации необходимо проводить с учётом предполагаемой вероятности возникновения угрозы и возможного ущерба от её осуществления.

Угрозы можно разделить на внешние и внутренние.

Угрозы объектам информационной безопасности проявляются *в виде:*

- разглашения конфиденциальной информации;
- утечки конфиденциальной информации через технические средства различного назначения;
- несанкционированного доступа к охраняемым информационным ресурсам;
- несанкционированного уничтожения и модификации информационных ресурсов;
- нарушения работы автоматизированных систем и сетей.

Источниками угроз могут быть:

- некомпетентность или халатность пользователей или персонала;
- злой умысел, независимо от того, внешним или внутренним относительно систем является источник угрозы;
- умышленное проникновение сторонних лиц в помещения, к аппаратуре и оборудованию;
- случайные события и стихийные бедствия.

Ситуация, возникающая в результате воздействия какой-либо угрозы, называется кризисной. Кризисные ситуации могу быть преднамеренными и непреднамеренными и иметь различную степень тяжести в зависимости от вызвавших их факторов риска, степени их воздействия, уязвимого места, категории информации.

Кризисные ситуации могут иметь следующие степени тяжести:

угрожающая - воздействие на объект информационной безопасности, которое может привести к полному выходу его из строя, а также уничтожение, модификацию или компрометацию (утечку) наиболее важной для Общества информации. Для устранения угрожающей ситуации требуется, как правило, полная или частичная замена оборудования, программ и данных;
серьезная - воздействие на объект информационной безопасности, которое может привести к выходу из строя отдельных компонентов, потере производительности, а также осуществлению несанкционированного доступа (НСД) к программам и данным. В этом случае система сохраняет работоспособность. Для устранения серьезной ситуации требуется, как правило, частичная замена (восстановление) оборудования, программ и данных, корректировка параметров системы, проведение организационно-технических мероприятий;
обычная - попытка воздействия на объект информационной безопасности, не наносящая ощутимого ущерба, но требующая реакции и расследования. Для устранения обычной ситуации, как правило, требуется корректировка параметров защиты.

7. ПОРЯДОК ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Работа по обеспечению ИБ в Обществе включает следующие этапы:
- определение информации содержащей коммерческую тайну и сроков ее действия;
- категорирование помещений по степени важности, обрабатываемой в них информации;
- определение категории информации обрабатываемой каждой отдельной системой;
- описание системы, определение факторов риска, определение уязвимых мест систем;
- выбор средств и мер защиты для предотвращения воздействия факторов риска и их минимизации;
- выбор средств и мер контроля и управления для своевременной локализации и минимизации воздействия факторов риска.

Отнесение информации к коммерческой тайне - установление ограничений на распространение информации, требующей защиты. Перечень сведений, относимых к категории коммерческой тайны определен Приказом по Обществу.

Отнесение информации к коммерческой тайне осуществляется в соответствии с принципами законности, обоснованности и своевременности. Обоснованность отнесения информации к коммерческой тайне заключается в установлении путем экспертной оценки

целесообразности защиты конкретных сведений исходя из жизненно - важных интересов Общества, вероятных финансовых и иных последствий нарушения режима соблюдения коммерческой тайны. Своевременность отнесения сведений к коммерческой тайне заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Категорирование помещений производится по степени важности обрабатываемой в них информации. В зависимости от категории обрабатываемой информации принимаются соответствующие меры по защите помещений.

Основная задача этапа *описания систем* - определение средств и непосредственных данных, подлежащих защите. В описание системы включаются:

- цели и задачи системы;
- пользователи и обслуживающий персонал;
- способы взаимодействия с другими системами как внутри Общества, так и с внешними объектами;
- физическую топологию сети в зданиях Общества;
- логическую топологию сети Общества, ее основные характеристики;
- перечень используемого оборудования, включая коммуникационное, периферийное, серверы, ПК, оборудование, их основные характеристики;
- перечень используемого программного обеспечения (системное, прикладное, коммуникационное) и его характеристики.

Описание системы должно проводиться с учетом организационной структуры подразделений, которые будут ее эксплуатировать.

Факторы риска — возможные ситуации, возникновение которых может расцениваться как угроза, и способные нанести ущерб материального или нематериального характера. Фактор риска оказывает воздействие на определенные участки объектов информационной безопасности и может учитываться или не учитываться в зависимости от степени воздействия на жизнедеятельность Общества.

Основными факторами риска являются:

- стихийные бедствия или чрезвычайные ситуации, приводящие к полному или частичному выходу из строя технических средств систем;
- несанкционированный доступ к серверам, элементам аппаратуры и оборудованию в серверных комнатах;
- неисправности и нарушения в функционировании программных и технических средств, отказ в санкционировании доступа к оборудованию, программам и данным, вызванные случайными сбоями или отказами;
- несанкционированные проникновения в информационно-вычислительную систему, в том числе по внешним каналам связи;
- мошенничество или умысел, а также некомпетентность или халатность, которые приводят к нарушению целостности или доступности информации;
- нарушение конфиденциальности отдельных данных;
- несанкционированный доступ к системным и прикладным данным и программам, а также ресурсам систем;
- повторное использование внешних и внутренних носителей информации для съема информации.

Перечень факторов риска может уточняться.

Уязвимые места - элементы технических средств, программ и данных, которые могут быть подвергнуты воздействию факторов риска. Уязвимые места необходимо защищать и контролировать.

К уязвимым местам объектов информационной безопасности относятся:
- все технические средства;
- все автоматизированные рабочие места (АРМ) и терминалы;
- все системное программное обеспечение и системные ресурсы, обеспечивающие функционирование автоматизированных систем и сетей Общества;
- опорная сеть Общества и передаваемые по ней данные;
- конфиденциальная и строго конфиденциальная информация;
- ресурсы и приложения систем, внутренние и внешние носители информации в системах, обрабатывающих конфиденциальную информацию;
Перечень уязвимых мест системы Общества может уточняться.

Для каждого конкретного объекта информационной безопасности осуществляется выбор конкретных средств и методов защиты, контроля и управления с учетом уязвимых мест и факторов риска.

8. ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ И СЕТЯХ

Основным объектом защиты является информация, циркулирующая в программно-аппаратных средствах, информационно-вычислительных системах и сетях, используемых в Обществе.

Основной целью обеспечения ИБ является защита АС и отдельных ее компонентов от воздействия факторов риска, а также минимизация воздействий от них.

В соответствии с Законом "Об информации, информационных технологиях и о защите информации" введено обязательное применение сертифицированных программно-аппаратных средств защиты информации. Поставщики средств должны иметь необходимые лицензии на распространение продукции и/или её обслуживание, а также иные лицензии в соответствии с законодательством РФ.

ИБ реализуется с помощью средств защиты и управления защитой, контроля и регистрации, обеспечения безотказной работы и восстановления систем и сетей.

Предотвращение кризисных ситуаций осуществляется средствами защиты, предохраняющими уязвимые места систем от воздействия факторов риска. В случае возникновения кризисных ситуаций, предотвращение которых средствами защиты невозможно, работа систем осуществляется по «Плану мероприятий по обеспечению непрерывной деятельности на случай непредвиденных обстоятельств» и по «Плану действий при возникновении чрезвычайных ситуаций».

ИБ достигается путем:
- предотвращения кризисных ситуаций, способных нанести ущерб программным и аппаратным средствам, информации, а также персоналу;
- минимизации ущерба и быстрейшего восстановления программных и аппаратных средств, информации, пострадавших в результате кризисных ситуаций, расследование причин и принятие соответствующих мер.

Меры по созданию режима защиты информационных ресурсов подразделяются на технические и организационно-правовые. При осуществлении технических мер применяются следующие средства защиты автоматизированных систем.
1. Средства контроля доступа и назначения полномочий:
- средства контроля доступа в помещения;

- средства идентификации и аутентификации при доступе к подсистемам программно-технических средств коллективного пользования;
- средства контроля доступа к серверам;
- средства контроля доступа к сети передачи данных;
- средства защиты на уровне ПК;
- средства протоколирования действий пользователей и обслуживающего персонала в системе.

2. Средства криптографической защиты информации (СКЗИ), применяемые для связи с внешними информационными, платежными и торговыми системами или для связи с клиентами.

Перечисленные средства необходимо использовать с учетом того, что каждый пользователь должен иметь минимум полномочий, необходимых и достаточных для решения своих задач. Применение данного принципа сводит к минимуму возможность НСД и облегчает расследование нарушений и фактов проникновения.

К организационно-правовым мероприятиям следует отнести наряду с общими обязательствами по сохранению коммерческой тайны, подписание специального обязательства о правилах пользования компьютерными сетями Общества. Отдельно оговариваются права на использование работником лицензионных программных продуктов, приобретаемых Обществом, и обязательства по порядку их использования и нераспространения.

Необходимым элементом обеспечения ИБ является однозначная идентификация (определение личности) и аутентификация (подтверждение личности) пользователей, применяемые в Обществе в виде парольной защиты. При этом требуется использовать обязательную парольную защиту в качестве базовой с предотвращением перехвата пароля. Пароль должен обновляться не реже 1 раза в 90 дней. (В соответствии с «Положением о парольной защите в информационных системах ООО «СПСР-ЭКСПРЕСС»)

Права доступа персонала к активам Общества распределяются в соответствии с заявкой непосредственного руководителя.

При работе с приложениями также используется механизм аутентификации для доступа к узлам или другой аппаратуре, обрабатывающей конфиденциальную информацию, использовать усиление парольной защиты в виде специальных программно-аппаратных средств.

Средства защиты серверов и каналообразующего телекоммуникационного оборудования предназначены для обеспечения конфиденциальности и целостности путем защиты от НСД к ЭВМ, среде исполнения процесса, областям пользователей, областям оперативной памяти и дискового пространства, данным на чтение/модификацию/уничтожение. Обеспечение доступности достигается средствами мониторинга и диагностики, а также с помощью средств и мер, обеспечивающих непрерывность работы.

Конкретные способы и методы использования средств защиты определяются особенностями конкретной системы или сервера и регламентируются планом защиты конкретной системы.

Телекоммуникационная сеть Общества представляет собой совокупность локальных сетей Общества, филиалов, обособленных подразделений и представительств, а также опорной сети Общества (сети провайдеров телекоммуникационных услуг). Основной задачей защиты телекоммуникационной сети является:

- обеспечение конфиденциальности передаваемой информации (предотвращение прослушивания трафика);

- целостность конфигурации и трафика сети;
- доступность ресурсов сети;
- контроль доступа для предотвращения НСД извне;
- контроль доступа и управления коммуникационным оборудованием локальной сети.

Задачи защиты сетей Общества решаются на основе существующих программно-аппаратных коммуникационных средств. Те задачи, которые не могут быть решены на уровне транспортной службы сети, должны решаться средствами операционных систем и приложений.

При входе в сеть общего пользования (Internet) применяются следующие меры по защите Внутренней сети:

- взаимодействие с сетью общего пользования осуществляется через специальный шлюз;
- если сеть общего пользования используется для передачи конфиденциальной информации, то такая передача должна осуществляться с применением средств криптозащиты;
- доступ работников Общества к сети общего пользования должен быть строго регламентирован.

Защита на уровне ПК является защитой рабочего места пользователя и одним из основных элементов комплексной защиты для однозначной идентификации «пользователь - рабочее место».

Средства защиты ПК должны обеспечивать:

- идентификацию и аутентификацию пользователя;
- невозможность изменения системных параметров компьютера, инсталляцию программного обеспечения, копирование данных на съемные носители информации;
- защиту системного и прикладного программного обеспечения, в том числе сетевого, от реконфигурации;
- отсутствие программ - вирусов и программ - закладок;
- невозможность физического доступа к аппаратным ресурсам ПК;
- запрет на применение считывающих устройств с внешних носителей информации, исключение делается для пользователей, имеющих разрешение Службы безопасности;
- ведение системного журнала по основным событиям;
- требование изменять установленные производителем настройки по умолчанию перед установкой системы в сетевую инфраструктуру (сменить установленные по умолчанию пароли, строки доступа, удалить ненужные для работы учетные записи).

На каждом рабочем месте должны быть зарегистрированы только два пользователя: непосредственно пользователь и администратор.

Криптографическая защита является единственно надежным средством защиты конфиденциальной информации при передаче по каналам связи. В каждой системе Общества используется, как правило, штатное программно-аппаратное средство криптозащиты.

Внутренний порядок применения СКЗИ в АС определяется «Положением об использовании средств криптографической защиты информации». Разработка Инструкций по применению СКЗИ и по обращению и хранению носителей ключевой информации, их своевременное обновление, а также контроль за исполнением Инструкций осуществляется ведущим специалистом по информационной безопасности. Контроль и учет использования СКЗИ осуществляет ведущий специалист по информационной безопасности.

Средства криптографической защиты информации поставляется разработчиками с полным комплектом эксплуатационной документации, включая описания ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения. Средства криптографической защиты информации имеют строгий регламент использования ключей, предполагающий контроль со стороны ведущего специалиста по информационной безопасности за действиями пользователя на всех этапах работы с ключевой информацией (получения ключевого носителя, ввод ключей, использование ключей и сдача ключевого носителя).

Доступ к ключам шифрования разрешен только ответственным за их хранение и использование работникам, назначаемым Приказом по Обществу. Ключи хранятся только в строго определенных защищенных хранилищах и строго определенном виде. Запрещатся хранить критичные аутентификационные данные после авторизации (даже в зашифрованном виде).

Помещения для размещения технических средств криптографической защиты информации находятся в зоне безопасности. Под зоной безопасности понимается территория Общества, в которой имеют право находиться только работники Общества, имеющие в неё допуск. Для доступа в помещение с регламентацией санкционированного права допуска используются системы контроля и учёта.

Главной задачей *средств контроля* является своевременное обнаружение и регистрация ситуаций, которые в соответствии с установленными факторами риска могут быть расценены как угрозы Обществу. Контроль включает в себя:

- регистрацию событий в целях профилактики информационной безопасности или же тех событий, которые могут быть расценены как угроза;
- выдачу соответствующих сообщений на консоль оператора или/и протоколирование параметров событий в системном журнале.

Данные электронные журналы доступны для чтения, анализа и резервного копирования только администратору соответствующего ПО, который несет персональную ответственность за полноту и точность отражения в журнале имевших место событий. Все журналы АС доступны для чтения ведущему специалисту по информационной безопасности, который осуществляет контроль использования информационных активов Общества.

Средства управления предназначены для оперативной реакции со стороны администраторов безопасности систем на различные, в т.ч. и кризисные ситуации, а также для настройки основных параметров системы.

Основными функциями управления являются:

- ликвидация аварийных ситуаций;
- конфигурирование программно-аппаратных средств подсистем;
- защита от НСД;
-регистрация пользователей и распределение ресурсов.

Организационные меры являются основным элементом, связывающим в единое целое средства и меры защиты, контроля и управления, а также правила их использования и применения. К организационным мерам относятся также разработка руководящих и нормативных документов и контроль за их выполнением.

9. ОБЕСПЕЧЕНИЕ АНТИВИРУСНОЙ ЗАЩИТЫ

Обеспечение антивирусной защиты в Обществе осуществляется в соответствии с Политикой антивирусной защиты информационной системы.

Установка и регулярное обновление средств антивирусной защиты на автоматизированных рабочих местах и серверах АС осуществляется администратором антивирусной защиты, назначенным Приказом по Обществу. На всех ЭВМ Общества настраивается автоматическая установка обновлений антивирусного программного обеспечения.

Антивирусное программное обеспечение развернуто на всех системах, подверженных воздействию вирусов (особенно рабочих станциях и серверах). Антивирусные механизмы должны быть актуальными, постоянно включенными и должны вести журналы протоколирования событий. На все системные компоненты и программное обеспечение устанавливаются самые свежие обновления безопасности, выпущенные производителем. Отключение антивирусных средств или отказ от автоматического обновления антивирусных баз не допускается.

Установка и обновление антивирусных средств контролируется работниками Дирекции по информационным технологиям.

Все факты модификации и разрушения данных на серверах или рабочих станциях, а также заражение их вирусами, классифицируются как значимые нарушения ИБ и могут стать предметом служебного расследования.

Ответственность за неисполнение или ненадлежащее исполнение требований антивирусной защиты возлагаются на каждого работника Общества, имеющего доступ к ЭВМ и/или АС.

10. ОРГАНИЗАЦИЯ БЕЗОТКАЗНОЙ РАБОТЫ

Для обеспечения безотказной работы и восстановления автоматизированных систем и сетей в случаях аварий, стихийных бедствий и других кризисных ситуаций, предусматриваются соответствующие меры и средства. Они составляют основу «Плана мероприятий по обеспечению непрерывной деятельности на случай непредвиденных обстоятельств»

Для обеспечения безотказной работы и восстановления сетей и систем помимо организационных мер используется специальное оборудование и процедуры:

- Бесперебойное электропитание - наиболее важный элемент обеспечения безотказной работы. Оно обеспечивается путем установки системы перехода на резервное питание при выходе из строя основного, установкой источников бесперебойного питания, дающих возможность системе функционировать до прибытия работников эксплуатационных служб и устранения аварии электропитания.
- Резервное копирование и хранение программ и данных на внешних носителях - основной способ их сохранения. Резервное копирование может быть полным (копии со всех данных) и выборочным (копии наиболее важных данных). Способ и периодичность резервного копирования определяется для каждой системы индивидуально. Целесообразно хранить несколько поколений данных и на каждую копию иметь дубликат, который должен храниться отдельно от основной копии в специальном оборудованном защищенном помещении Общества на значительном удалении от действующей системы.
- Резервирование аппаратных ресурсов - применяется для обеспечения восстановления работоспособности системы при отказах аппаратных средств.

Основным критерием использования резервных ресурсов является критичность по отношению к жизнедеятельности Общества и экономическая целесообразность. Наиболее уязвимыми элементами системы являются серверы, используемые для работы систем,

каналообразующее телекоммуникационное оборудование и каналы связи. В связи с этим целесообразно применять отказоустойчивые серверы и коммуникационное оборудование, в которых конструктивно резервируются и дублируются наиболее критичные элементы.

Для наиболее важных систем используется «холодный резерв» - второй комплект оборудования. Для обеспечения функционирования систем при обмене данными по внешним сетям, необходимо предусмотреть резервирование каналов связи и коммуникационного оборудования, в том числе разных поставщиков телекоммуникационных услуг (провайдеров).

Помимо мер по предотвращению возникновения кризисных ситуаций предусмотрены организационные мероприятия для устранения их последствий, которые включают в себя:

- локализацию области воздействия фактора риска;
- уведомление соответствующих должностных лиц о факте возникновения кризисной ситуации;
- предотвращение расширения кризисной ситуации, при необходимости выведение из эксплуатации системы, комплексов или отдельных компонентов;
- обеспечение безотказной работы, оперативную корректировку параметров системы, удаление или выведение из эксплуатации пораженных элементов системы, загрузку копий программного обеспечения и/или переход на резервное оборудование;
- полное устранение причин кризисной ситуации;
- восстановление аппаратных, программных и информационных элементов систем;
- расследование причин кризисной ситуации, пересмотр плана защиты (при необходимости).

Для определения действий в кризисных ситуациях в целях обеспечения безотказной работы и восстановления функционирования систем разработан и утвержден «План мероприятий по обеспечению непрерывной деятельности на случай непредвиденных обстоятельств». Кризисные ситуации, не предусмотренные Планом, считаются случайными и отвечающими допустимому уровню риска.

Кризисные ситуации, возникающие в результате несоответствия технической документации поставленному в Обществ продукту (оборудованию, программному обеспечению), рассматриваются как случайные угрозы, ответственность за которые несет разработчик. Для минимизации воздействия недокументированных свойств принимаются следующие меры:

- по всем АС имеются договоры поддержки с фирмами-производителями или распространителями;
- до заключения договоров с разработчиками на поставку ПО, а также на проведение пусконаладочных работ или работ по внедрению программно-аппаратных решений сторонами должны быть подписаны соглашения о соблюдении режима конфиденциальности, куда вносится пункт об ответственности за недокументированные свойства разработок;
- периодическая проверка состояния системного и прикладного ПО на предмет диагностики штатного состояния.

Надежность средств защиты, контроля и управления, призванных обеспечить ИБ, определяется на основе технических и эксплуатационных характеристик средств, внесённых в документацию и подтвержденных тестированием.

11. ИСПОЛЬЗОВАНИЕ РЕСУРСОВ СЕТИ ИНТЕРНЕТ

Ресурсы сети Интернет в Обществе используются для ведения дистанционного обслуживания клиентов, получения и распространения информации, связанной с

деятельностью Общества, информационно-аналитической работы в интересах Общества, обмена почтовыми сообщениями с клиентами и партнерами, а также ведения собственной хозяйственной деятельности. Любое иное использование ресурсов сети Интернет, решение о котором не принято руководством Общества в установленном порядке, рассматривается как нарушение ИБ.

Порядок подключения и использования ресурсов сети Интернет регламентируется «Регламентом использования сети Интернет и электронной почты».

Подключение пользователей к сети Интернет производится администратором системы только при наличии надлежащим образом оформленной заявки на подключение.

Для контроля трафика в Обществе установлена система, учитывающая объем и содержание трафика каждого пользователя.

Статистика посещений ресурсов Интернета архивируется и хранится в течение шести месяцев. Полная статистика в целом по Обществу доступна только администратору системы учета трафика. Изменения в архиве не допускаются. Администратор системы учета трафика предоставляет руководителям структурных подразделений по их запросу отчет о статистике посещений работников своего подразделения за указанный в запросе период.

12. ЗАЩИТА РЕЧЕВОЙ ИНФОРМАЦИИ

Основной целью защиты конфиденциальной речевой информации является предотвращение несанкционированного съёма информации по всевозможным каналам, которые могут иметь естественный характер или создаваться преднамеренно. Защита речевой информации представляет собой процесс, организуемый и поддерживаемый в Обществе с целью предупреждения ее утечки. Непосредственные работы по защите речевой информации проводит Служба безопасности.

Возможными каналами утечки речевой информации являются:
- умышленное или неумышленное разглашение работниками Общества сведений, отнесённых к коммерческой тайне;
- радиолинии телефонной связи;
- линии проводной телефонной связи;

Каналы утечки могут быть естественные и искусственные. Естественные каналы существуют в Обществе и для трансляции снимаемых сигналов не требуются какие-либо «закладные» технические средства. Искусственные каналы (с использованием внедренных технических устройств) создаются преднамеренно.

Противодействие утечке речевой информации представляет собой систему мер, направленную на выявление естественных и искусственных каналов утечки и предотвращению утечки по этим каналам. Противодействие должно носить непрерывный и плановый характер.

Меры противодействия утечки речевой информации делятся на административные и организационно-технические.

Административные меры:

- проведение категорирования служебных помещений Общества, в том числе в филиалах, обособленных подразделениях и представительствах;
- разработка инструкций по защите коммерческой тайны при проведении деловых встреч и переговоров, ведении телефонных разговоров и контроль их выполнения;
- разработка нормативных документов по порядку проведения обследований служебных помещений и технических средств на предмет определения естественных и искусственных каналов утечки;
- обеспечение режима доступа в служебные помещения.

Организационно-технические меры:

- проведение специальных обследований служебных помещений и технических средств;
- проведение специальных обследований строящихся и ремонтируемых зданий и помещений;
- приобретение специальных технических средств обнаружения каналов утечки и их закрытия, организация учета и контроля их использования;
- оборудование категорированных помещений специальными средствами защиты от утечки информации;
- оборудование служебных помещений средствами разграничения доступа.

13. ОРГАНИЗАЦИЯ ФИЗИЧЕСКОГО ДОСТУПА К ДАННЫМ И ИХ ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ.

В связи с тем, что физический доступ к системам, предоставляет возможность получить контроль над устройствами и данными, а также украсть устройство или документ, он должен быть соответствующим образом ограничен.

Для ограничения и отслеживания физического доступа к системам, которые хранят, обрабатывают или передают данные, используются средства контроля доступа в помещение, такие как: камеры видеонаблюдения, ограничения доступа к сетевым разъемам, к беспроводным точкам доступа, шлюзам и портативным устройствам, расположенным в общедоступных местах.

Оборудование (серверы, рабочие станции, ноутбуки) и носители, содержащие данные держателей, физически защищены от несанкционированного доступа.

В целях данного ограничения доступа, а также контроля доступа в помещения Общества, где хранится, обрабатывается или передается информация, принимаются следующие меры и действия:

- Все помещения, на территории которых имеются помещения, где циркулируют данные, имеют круглосуточную физическую охрану, оснащены системами пультовой охраны и видеонаблюдения.
- Доступ в аппаратные имеет только технический персонал обслуживающий аппаратуру с круглосуточным режимом работы. Список этих лиц утверждается Приказом по Обществу.

Доступ посетителей (привлечение сторонних лиц, для каких либо ремонтных работ) осуществляется после их регистрации в журнале учета, и только в сопровождении технического персонала ИТ.

Помещения оснащены металлическими дверями с надежными запирающими устройствами. Ключи от аппаратных в опечатанных контейнерах хранятся на посту охраны Общества.

Помещения оборудованы системами автоматизированного контроля доступа и видеонаблюдения с постоянной записью информации на выделенный специализированный сервер

Помещения имеют повышенную категорию защиты на пожарную опасность и оснащены автоматизированной системой пожаротушения.

Обществом определены процедуры, позволяющие различать работников и посетителей, особенно в помещениях, где циркулируют конфиденциальные данные. Под термином «работники» в данном случае понимаются постоянные и временные работники, а также консультанты, работающие на объекте. Под термином «посетители» понимаются поставщики, сервисный персонал и иные люди, кратковременно находящиеся на объекте, обычно не более одного дня.

Обществом внедрены процедуры прохода посетителей на объект, обеспечивающие:

- авторизацию посетителя, перед входом в помещения, где имеются конфиденциальные данные;
- выдачу посетителю материального идентификатора имеющего ограничение срока действия, при входе на объект;
- возвращение посетителем выданного материального идентификатора при выходе с объекта или при истечении его срока действия.

Имеющийся множественный контроль физической безопасности (бэйджи, сопровождение) предупреждает возможность беспрепятственного неавторизованного прохода в помещения, где имеются конфиденциальные данные;

В Обществе ведется журнал учета посетителей, который хранится не менее 3 (Трех) месяцев.

Физическая безопасность всех бумажных и электронных средств (включая компьютеры, электронные носители информации, сетевое оборудование, линии телекоммуникаций, бумажные отчеты, чеки и факсимильные сообщения), содержащих конфиденциальные данные обеспечиваются путем строго контроля над перемещением носителей информации с доверенным курьером, или иным способом, который может быть тщательно проконтролирован.

Носители информации с конфиденциальными данными, могут быть уязвимы по отношению к несанкционированному доступу, использованию и повреждению во время транспортировки из одного офиса в другой.

Для защиты носителей конфиденциальной информации во время транспортировки, необходимо осуществлять следующие меры и средства контроля:

- утвердить список курьеров, наделённых соответствующими полномочиями;
- утвердить маршруты движения;
- в журнале учёта перемещений носителей информации делается запись, подробно расшифровывающая: классификацию носителей информации, их маркировку, как содержащих конфиденциальную информацию, кем, когда и куда перевозился и кем был принят;
- для обеспечения надлежащей защиты носителя, от возможного физического повреждения во время транспортировки необходимо применение упаковки контейнерного типа, защищённой от постороннего вмешательства (которое позволяет выявить попытки её вскрытия);
- в исключительных случаях предусмотрено разделение особо секретной информации на несколько частей, с её помещением на разных носителях с целью их транспортировки разными маршрутами.

Работникам Общества запрещается выносить оборудование, различные носители информации (не содержащие конфиденциальную информацию) за пределы помещения без письменного разрешения руководства.

В случае необходимости перемещения какого-либо оборудования или имущества:

- начальником подразделения готовиться служебная записка с указанием наименования имущества, его количества и место куда перемещается;
- начальник визирует заявку на вынос имущества;
- данная заявка служит для работников охраны пропуском на вынос и остаётся на посту охраны, где учитывается в журнале.

Носители информации, находящиеся на рабочих столах, могут быть прочитаны, скопированы или повреждены. Для предупреждения утраты или несанкционированного копирования применяются следующие меры:

- носителям, содержащим конфиденциальные данные, обеспечена физическая безопасность;
- бумажная документация и носители, когда они не используются, должны храниться в специальных шкафах, особенно в нерабочее время;
- конфиденциальная или критически важная информация, когда она не используется, должна храниться отдельно (в сейфе или несгораемом шкафу), особенно в нерабочее время.

Непосредственный процесс уничтожения носителей конфиденциальной информации осуществляет комиссия, созданная Приказом по Обществу. По окончании уничтожения составляется акт, который хранится у руководителя подразделения.

Носители, содержащие конфиденциальные данные, хранение которых более не требуется для выполнения бизнес-задач или требований законодательства уничтожаются следующими способами:
- измельчение, сжигание или растворение бумажного носителя;
- очищение, размагничивание, измельчение или иное разрушение электронного носителя, исключающее возможность восстановления данных о держателях карт.

Кроме того, в целях соблюдения Политики ИБ принимаются упреждающие меры, такие как:

Работники при приеме на работу в Общество подписывают обязательство о неразглашении коммерческой тайны Общества. В данном документе освещаются вопросы, связанные с информационной безопасностью и сопутствующими с ними процедурами.

Приказом, изданным за подписью Генерального директора Общества, утвержден «Кодекс корпоративной этики ООО «СПСР-ЭКСПРЕСС».

В филиалах, обособленных подразделениях и представительствах Приказом по обществу назначаются ответственные за обеспечение ИБ.

В отношении работников Общества, в том числе имеющих доступ к системам, которые хранят, обрабатывают или передают конфиденциальные данные, Службой безопасности Общества проводится регулярная проверка их благонадежности.

14. ИБ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ ОБЩЕСТВА

Система обеспечения ИБ информационного технологического процесса Общества соответствует требованиям настоящей Политики и иных нормативных документов по вопросам ИБ.

В Обществе информация классифицируется как:

- открытая информация, предназначенная для официальной передачи во внешние организации и средства массовой информации;
- внутренняя информация, предназначенная для использования исключительно работниками Общества при выполнении ими своих служебных обязанностей;
- информация, содержащая сведения ограниченного распространения в соответствии с утвержденным в Обществе Перечнем информации, относящейся к коммерческой тайне в соответствии с законодательством РФ.

Для каждой АС Приказом назначаются администраторы системы, ответственные за ее работу.

По решению Генерального директора Общества для защиты информации, обрабатываемой в различных АС, могут назначаться администраторы ИБ. Функции, права и обязанности администратора ИБ каждой АС определяются соответствующим Приказом Президента Общества. Допускается назначение одного администратора ИБ на несколько подсистем, а также совмещение выполнения указанных функций с другими обязанностями.

В случае использования внешних информационных систем или аутсорсинга вопросы администрирования и обеспечения ИБ в этой системе явно описываются в Договоре.

Администратор АС не имеет служебных полномочий и технических средств для администрирования пользователей сети, в среде которой работает АС (добавление нового пользователя, удаление действующего пользователя и корректировка прав и полномочий действующего пользователя). Администратор сети не имеет служебных полномочий и технических средств для администрирования пользователей АС (добавление нового пользователя, удаление действующего пользователя и корректировка прав и полномочий действующего пользователя).

Администратор ИБ контролирует соответствие назначенных прав доступа пользователей к АС указанным в разрешительных документах.

Процессы подготовки, ввода, обработки и хранения информации, а также порядок установки, настройки, эксплуатации и восстановления необходимых технических и программных средств регламентируются и обеспечиваются инструктивными и методическими материалами.

С целью контроля исполнения мероприятий по ИБ в Обществе осуществляется периодическое тестирование всех реализованных программно-техническими средствами функций (требований) по обеспечению ИБ.

В Обществе разрабатывается и реализуется процедура восстановления системы обеспечения ИБ после технических сбоев или преднамеренных атак.

15. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДОКУМЕНТООБОРОТА

Обеспечение информационной безопасности документооборота осуществляется в соответствии с Инструкцией по делопроизводству.

16. РАСПРЕДЕЛЕНИЕ ФУНКЦИЙ ПО ОБЕСПЕЧЕНИЮ ИБ МЕЖДУ ПОДРАЗДЕЛЕНИЯМИ И ДОЛЖНОСТНЫМИ ЛИЦАМИ.

Процедура управления ИБ Общества включает в себя:

- разработку политики информационной безопасности;
- разработку нормативно-методических документов обеспечения ИБ;
- обеспечение штатного функционирования комплекса средств ИБ Общества;
- осуществление контроля (мониторинга) функционирования системы ИБ Общества;
- обучение с целью поддержки (повышения) квалификации персонала Общества;
- оценку рисков, связанных с нарушениями ИБ.

Для реализации этих задач в Службе безопасности Общества предусмотрена должность ведущего специалиста по информационной безопасности, в обязанности которого входит:

- определение характера угроз и разработка предложений по изменению политики ИБ Общества;
- разработка предложений по изменению существующих и принятию новых нормативно-методических документов по обеспечению ИБ Общества;
- определение минимально необходимого набора технических средств, критически важных для функционирования Общества в условиях технических сбоев, аварий перебоях в электропитании, и разработка мер по обеспечению их безотказной работы;
- контроль доступа пользователей к информационным активам;
- контроль функционирования средств обеспечения ИБ;
- контроль работников Общества, в части выполнения ими требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь, работников, имеющих максимальные полномочия по доступу к защищаемым информационным активам;
- осуществление мониторинга событий, связанных с ИБ;

- расследование событий, связанные с нарушениями ИБ, и разработка мер, исключающих подобные события в будущем.

- участие в восстановлении работоспособности АС, анализ причин технических сбоев и аварий и разработка мер по их предотвращению.

Распределение функций по обеспечению ИБ между подразделениями и должностными лицами:

Дирекция по информационным технологиям:

Основными функциями по обеспечению ИБ, выполняемыми Дирекцией по ИТ, являются:

- согласование проектов всех внутренних документов, затрагивающих вопросы безопасности технологий, используемых в Обществе;
- администрирование информационных ресурсов АС Общества в части обеспечения работоспособности системного и прикладного программного обеспечения и их обновления,
- обеспечение бесперебойной работы АС Общества и оперативное восстановление их работы после сбоев,
- обеспечение системы защиты АС Общества необходимыми программно – аппаратными средствами,
- создание и сопровождение фонда алгоритмов и программ,
- обучение пользователей АС безопасной работе с информационными активами.
- осуществление контроля функционирования системы ИБ Общества;
- разработка технических заданий, проектирование, создание, тестирование и приемка средств и систем защиты АС;
- подключение и использование ресурсов сети Интернет, контроль трафика;
- мониторинг сообщений о работе электронной почты.

Служба безопасности:

- разработка и реализация мер физической защиты информационных ресурсов (охранная и пожарная сигнализация, охрана зданий и помещений, видеонаблюдение и т.п.);
- контроль выполнения требований информационной безопасности в части оборудования и эксплуатации режимных помещений;
- участвует в расследовании случаев несанкционированного доступа к АС или попыток такого доступа;
- организация мероприятий по профилактике и выявлению нарушений требований информационной безопасности, связанных с нарушением конфиденциальности сведений, составляющих коммерческую тайну, финансовых потерь и ущерба деловой репутации Общества;

Дирекция управления персоналом:

- ведение кадрового делопроизводства, обеспечение учета и хранения персональных данных работников и соискателей, применение кадровых технологий в соответствии с требованиями информационной безопасности;
- разработка и реализация процедурных мер защиты информации, включая организацию соответствующего подбора и обучения кадров;

Юридический отдел:

- разработка и реализация правовых мер защиты информации;
- разработка технологий подготовки, ведения и хранения договоров, организации взаимоотношений с клиентами, контрагентами и партнерами, с другими внешними организациями в соответствии с требованиями информационной безопасности (совместно со Службой безопасности);

Делопроизводство:

- осуществляет регистрацию и рассылку в сторонние организации защищаемой информации на бумажных носителях,
- осуществляет централизованную регистрацию носителей ключевой информации.

Руководители подразделений:

- контролируют безопасность работы с информацией подчиненными работниками,
- обеспечивают соблюдение работниками положений Политики информационной безопасности, других документов по ИБ.

17. ПОРЯДОК УТВЕРЖДЕНИЯ, ВНЕСЕНИЯ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ.

Настоящая Политика ИБ вступает в силу с даты утверждения.

В случае вступления отдельных пунктов в противоречие с новыми законодательными актами, эти пункты утрачивают юридическую силу до момента внесения изменений в настоящую Политику ИБ.

Пересмотр Политики информационной безопасности производится не реже одного раза в год и имеет целью приведение в соответствие определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации.